Оценка глубины обратимых схем из функциональных элементов NOT, CNOT и 2-CNOT

Д. В. Закаблуков*

16 февраля 2016 г.

Аннотация

Рассматривается вопрос об асимптотической глубине обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. Вводится функция Шеннона $D(n, q)$ глубины обратимой схемы, реализующей какое-либо отображение $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, как функция от n и количества дополнительных входов схемы q. Доказывается, что при реализации отображения f, задающего четную подстановку на множестве $\mathbb{Z}_2^n$, обратимой схемой, не использующей дополнительные входы, верно соотношение $D(n, 0) \gtrsim 2^n/(3\log_2 n)$. Устанавливается также, что при использовании $q_0 \sim 2^n$ дополнительных входов для реализации произвольного отображения $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ в обратимой схеме верно соотношение $D(n, q_0) \lesssim 3n$.

Ключевые слова: обратимые схемы, глубина схемы, вычисления с памятью.

1. Введение. В дискретной математике нередко возникает задача оценивания асимптотической сложности того или иного преобразования. Теория схемной сложности берет свое начало с работы К. Шеннона [1]. В ней в качестве меры сложности булевой функции предлагается рассматривать сложность минимальной контактной схемы, реализующей эту функцию. О. Б. Лупановым [2] установлена асимптотика сложности $L(n) \sim \rho 2^n / n$ булевой функции от n переменных в произвольном конечном полном базисе элементов с произвольными положительными весами, где ρ обозначает минимальный приведенный вес элементов базиса.

Вопрос о вычислениях с ограниченной памятью был рассмотрен Н. А. Карповой в работе [3], где доказано, что в базисе классических функциональных элементов, реализующих все p-местные булевы функции, асимптотическая оценка функции Шеннона сложности схемы с тремя и более регистрами памяти зависит от значения p, но не изменяется при увеличении количества используемых регистров памяти. Также было показано, что существует булева функция, которая не может быть реализована в маломестных базисах с использованием менее двух регистров памяти.

* *Закаблуков Дмитрий Владимирович* — асп. каф. информационной безопасности ф-та информатики и систем управления МГТУ им. Н. Э. Баумана, e-mail: dmitriy.zakablukov@gmail.com.

О. Б. Лупановым в работе [4] рассмотрены схемы из функциональных элементов с задержками. Было доказано, что в регулярном базисе функциональных элементов любая булева функция может быть реализована схемой, имеющей задержку $T(n) \sim \tau n$, где τ — минимум приведенных задержек всех элементов базиса, при сохранении асимптотически оптимальной сложности. Однако не рассматривался вопрос зависимости $T(n)$ от количества используемых регистров памяти. Хотя задержка и глубина схемы в некоторых работах определяются по-разному [5], в исследуемой далее модели обратимой схемы их, по мнению автора, можно отождествить.

В настоящей работе рассматриваются схемы, состоящие из обратимых функциональных элементов NOT (инвертор), 1-CNOT (контролируемый инвертор, CNOT) и 2-CNOT (дважды контролируемый инвертор, элемент Тоффоли). Будут использоваться формальные определения этих элементов и состоящих из них схем из работы [6]. В [7, 8] доказано, что для любой четной подстановки $h \in A(\mathbb{Z}_2^n)$ существует задающая ее обратимая схема с n входами, состоящая из элементов NOT, CNOT и 2-CNOT.

В работе [9] рассматривались обратимые схемы без дополнительных входов (дополнительной памяти), состоящие из обобщенных элементов Тоффоли k-CNOT; была установлена нижняя оценка функции Шеннона сложности таких схем $L(n) > \frac{n2^n}{\log_2 n+n-1}$. В [7] также рассматривались обратимые схемы без дополнительных входов, но уже в базисе NOT, CNOT и 2-CNOT; были доказаны нижняя оценка функции Шеннона сложности таких схем $L(n) = \Omega\left(\frac{n2^n}{\log_2 n}\right)$ и верхняя оценка $L(n) \leqslant O(n2^n)$. В [10] была улучшена верхняя оценка: $L(n) \lesssim 5n2^n$. Однако схемы с дополнительными входами в данных работах не рассматривались.

В работе [11] было доказано, что для функции Шеннона сложности обратимых схем без дополнительных входов, состоящих из элементов NOT, CNOT и 2-CNOT, верно соотношение $L(n) \asymp \frac{n2^n}{\log_2 n}$. Также было показано, что использование дополнительной памяти в таких схемах почти всегда позволяет снизить сложность схемы.

Автору не удалось найти какие-либо опубликованные результаты об оценке функции Шеннона глубины обратимых схем, состоящих из элементов NOT, CNOT и 2-CNOT. Тем не менее в работе [12] было экспериментально показано, что использование $O(n)$ дополнительных входов позволяет значительно снизить глубину таких схем.

В настоящей работе рассматривается множество $F(n, q)$ всех отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$, которые могут быть реализованы обратимой схемой, состоящей из элементов NOT, CNOT и 2-CNOT (далее просто обратимая схема), с $(n+q)$ входами. Оценивается глубина обратимой схемы, реализующей отображение $f \in F(n, q)$ с использованием q дополнительных входов. Вводится функция Шеннона $D(n, q)$ глубины обратимой схемы как функция от n и количества дополнительных входов схемы q. Показывается, что, как и в случае сложности обратимой схемы [11], глубина обратимой схемы существенно зависит от количества дополнительных входов (регистров памяти, см. [3]).

При помощи мощностного метода Риордана–Шеннона доказывается нижняя оценка глубины обратимой схемы $D(n, q) \geqslant (2^n(n-2) - n\log_2(n+q))/(3(n+q)\log_2(n+q))$. Описывается аналогичный методу О. Б. Лупанова [4] подход к синтезу обратимой схемы, для которого глубина синтези-

рованной схемы $D(n, q_0) \lesssim 3n$ при использовании $q_0 \sim 2^n$ дополнительных входов.

2. Основные понятия. Определение обратимых функциональных элементов было впервые введено Т. Тоффоли [13]. Обратимые функциональные элементы NOT и k-CNOT, а также синтез схем из этих элементов были рассмотрены, к примеру, в работе [14].

Будем пользоваться следующим формальным определением функциональных элементов NOT и k-CNOT [6]. Через N_j^n обозначается функциональный элемент NOT (инвертор) с n входами, задающий преобразование $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ вида

$$N_j^n(\langle x_1, \ldots, x_n \rangle) = \langle x_1, \ldots, x_j \oplus 1, \ldots, x_n \rangle \,. \tag{1}$$

Через $C^n_{i_1,\ldots,i_k;j} = C^n_{I;j}$, $j \notin I$, обозначается функциональный элемент k-CNOT с n входами (контролируемый инвертор, обобщенный элемент Тоффоли с k контролирующими входами), задающий преобразование $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ вида

$$C^n_{i_1,\ldots,i_k;j}(\langle x_1, \ldots, x_n \rangle) = \langle x_1, \ldots, x_j \oplus x_{i_1} \wedge \ldots \wedge x_{i_k}, \ldots, x_n \rangle \,. \tag{2}$$

Далее будем опускать верхний индекс n, если его значение ясно из контекста. Обозначим через Ω_n^2 множество всех функциональных элементов NOT, CNOT и 2-CNOT с n входами.

Схема из функциональных элементов классически определяется как ориентированный граф без циклов с помеченными ребрами и вершинами. В обратимых схемах, состоящих из элементов множества Ω_n^2, запрещено ветвление и произвольное подключение входов и выходов функциональных элементов. В ориентированном графе, описывающем такую обратимую схему $\mathfrak{S}$, все вершины, соответствующие функциональным элементам, имеют ровно n занумерованных входов и выходов. Эти вершины нумеруются от 1 до l, при этом i-й выход m-й вершины, $m < l$, соединяется только с i-м входом $(m+1)$-й вершины. Входами обратимой схемы являются входы первой вершины, а выходами — выходы l-й вершины. Соединение функциональных элементов друг с другом будем также называть композицией элементов.

Всем i-м входам и выходам вершин графа приписывается символ r_i из некоторого множества $R = \{\, r_1, \ldots, r_n \,\}$. Каждый символ r_i можно интерпретировать как имя регистра памяти (номер ячейки памяти), хранящего текущий результат работы схемы. Из формул (1) и (2) следует, что в один момент времени (один такт работы схемы) может быть инвертировано значение не более чем в одном регистре памяти. В этом заключается существенное отличие обратимых схем от схем из классических функциональных элементов, рассмотренных О. Б. Лупановым в своих работах.

Среди основных характеристик обратимой схемы можно выделить сложность и глубину схемы. Пусть обратимая схема $\mathfrak{S}$ с n входами представляет собой композицию l элементов из множества Ω_n^2: $\mathfrak{S} = \underset{j=1}{\overset{l}{*}} E_j(t_j, I_j)$, где t_j и I_j — контролируемый выход и множество контролирующих входов элемента E_j соответственно. Сложность $L(\mathfrak{S})$ обратимой схемы $\mathfrak{S}$ — количество элементов в схеме l. Классически глубина схемы из функциональных элементов определяется как длина максимального пути на графе, описывающем данную схему, между какими-либо входными и выходными вершинами. В рассматриваемой модели обратимой схемы граф, описывающий

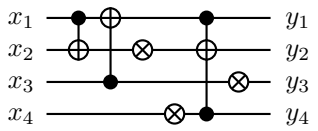

Рис. 1: Обратимая схема $\mathfrak{S} = C_{1;2} * C_{3;1} * N_2 * N_4 * C_{1,4;2} * N_3$ со сложностью $L(\mathfrak{S}) = 6$ и глубиной $D(\mathfrak{S}) = 3$

такую схему, представляет собой просто одну цепочку последовательно соединенных вершин. Поэтому, если использовать классическое определение глубины схемы, получится, что в нашем случае глубина обратимой схемы равна ее сложности.

Для того чтобы не менять модель обратимой схемы, введем следующее определение глубины обратимой схемы. Будем считать, что обратимая схема $\mathfrak{S} = \underset{j=1}{\overset{l}{*}} E_j(t_j, I_j)$ имеет глубину $D(\mathfrak{S}) = 1$, если для любых двух ее функциональных элементов $E_1(t_1, I_1)$ и $E_2(t_2, I_2)$ выполняется равенство

$$(\{\, t_1 \,\} \cup I_1) \cap (\{\, t_2 \,\} \cup I_2) = \varnothing \ .$$

Также будем считать, что обратимая схема $\mathfrak{S}$ имеет глубину $D(\mathfrak{S}) \leqslant d$, если ее можно разбить на d непересекающихся подсхем, каждая из которых имеет глубину 1:

$$\mathfrak{S} = \bigsqcup_{i=1}^{d} \mathfrak{S}'_i \ , \ D(\mathfrak{S}'_i) = 1 \ . \tag{3}$$

Тогда можно ввести следующее определение: глубина $D(\mathfrak{S})$ обратимой схемы $\mathfrak{S}$ — минимально возможное количество d непересекающихся подсхем глубины 1 в разбиении схемы $\mathfrak{S}$ по формуле (3). Используя это определение, можно вывести простое соотношение, связывающее сложность и глубину обратимой схемы $\mathfrak{S}$, имеющей n входов:

$$\frac{L(\mathfrak{S})}{n} \leqslant D(\mathfrak{S}) \leqslant L(\mathfrak{S}) \ . \tag{4}$$

На рис. 1 показан пример обратимой схемы со сложностью 6 и глубиной 3. На данном и на всех последующих рисунках элементы k-CNOT обозначаются следующим образом: контролирующие входы обозначаются символом $\bullet$, контролируемый выход — символом $\oplus$. Инвертируемый выход элемента NOT обозначается символом $\otimes$. Входы схемы/элементов, если не оговорено иначе, находятся слева, выходы — справа. Входы и выходы пронумерованы сверху вниз начиная с 1. Элементы в схеме соединяются без ветвлений входов и выходов, i-й выход j-го элемента соединяется с i-м входом $(j+1)$-го элемента. На входы обратимой схемы подаются значения 0 и 1, затем последовательно, слева направо, каждый из элементов инвертирует либо не инвертирует значение на одном (и только одном) из своих выходов в зависимости от значений на своих входах (см. формулы (1) и (2)).

3. Глубина обратимой схемы. Введем следующие отображения:

1) *расширяющее* отображение $\phi_{n,n+k} \colon \mathbb{Z}_2^n \to \mathbb{Z}_2^{n+k}$ вида

$$\phi_{n,n+k}(\langle x_1, \ldots, x_n \rangle) = \langle x_1, \ldots, x_n, 0, \ldots, 0 \rangle \ ;$$

2) *редуцирующее* отображение $\psi^{\pi}_{n+k,n}\colon \mathbb{Z}_2^{n+k} \to \mathbb{Z}_2^n$ вида

$$\psi^{\pi}_{n+k,n}(\langle x_1, \ldots, x_{n+k}\rangle) = \langle x_{\pi(1)}, \ldots, x_{\pi(n)}\rangle \ ,$$

где π — некоторая подстановка на множестве $\mathbb{Z}_{n+k}$.

Известно, что обратимая схема с $n \geqslant 4$ входами задает некоторую четную подстановку на множестве $\mathbb{Z}_2^n$ [7, 8]. В тоже время данная схема может реализовывать не более A_n^m (количество размещений из n по m без повторений) различных булевых отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$, где $m \leqslant n$, с использованием или без использования дополнительных входов. Введем формальное определение обратимой схемы, реализующей некоторое отображение $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ с использованием дополнительных входов.

Определение 1. Обратимая схема $\mathfrak{S}_g$ с $(n+q)$ входами, задающая преобразование $g\colon \mathbb{Z}_2^{n+q} \to \mathbb{Z}_2^{n+q}$, *реализует* отображение $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ с использованием $q \geqslant 0$ дополнительных входов (дополнительной памяти), если существует такая подстановка $\pi \in S(\mathbb{Z}_{n+q})$, что

$$\psi^{\pi}_{n+q,m}(g(\phi_{n,n+q}(\mathbf{x}))) = f(\mathbf{x}), \text{ где } \mathbf{x} \in \mathbb{Z}_2^n, f(\mathbf{x}) \in \mathbb{Z}_2^m \ .$$

Выражения «реализует отображение» и «задает отображение» имеют различное значение: если обратимая схема $\mathfrak{S}_g$ задает отображение f, то $g(\mathbf{x}) = f(\mathbf{x})$. Будем говорить, что схема $\mathfrak{S}_g$ реализует отображение f *без использования дополнительной памяти*, если она имеет ровно n входов. Очевидно, что при $m > n$ не существует обратимой схемы, реализующей отображение f без использования дополнительной памяти.

Обозначим через $P_2(n,n)$ множество всех булевых отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Обозначим через $F(n,q) \subseteq P_2(n,n)$ множество всех отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$, которые могут быть реализованы обратимой схемой с $(n+q)$ входами. Множество подстановок из $S(\mathbb{Z}_2^n)$, задаваемых всеми элементами множества Ω_n^2, генерирует знакопеременную $A(\mathbb{Z}_2^n)$ и симметрическую $S(\mathbb{Z}_2^n)$ группы подстановок при $n > 3$ и $n \leqslant 3$ соответственно [7, 8]. Отсюда следует, что $F(n,0)$ совпадает с множеством преобразований, задаваемых всеми подстановками из $A(\mathbb{Z}_2^n)$ и $S(\mathbb{Z}_2^n)$ при $n > 3$ и $n \leqslant 3$ соответственно. С другой стороны, несложно показать, что при $q \geqslant n$ верно равенство $F(n,q) = P_2(n,n)$.

Обозначим через $L(f,q)$ и $D(f,q)$ минимальную сложность и глубину обратимой схемы, состоящей из функциональных элементов множества Ω^2_{n+q} и реализующей некоторое отображение $f \in F(n,q)$ с использованием q дополнительных входов. Определим функции Шеннона $L(n,q)$ и $D(n,q)$ для сложности и глубины обратимой схемы:

$$L(n,q) = \max_{f \in F(n,q)} L(f,q) \ , \quad D(n,q) = \max_{f \in F(n,q)} D(f,q) \ .$$

Сформулируем основные результаты работы. Доказательство приведенных ниже теорем будет дано в следующих пунктах. Будем использовать следующие обозначения для асимптотического неравенства, эквивалентности и эквивалентности с точностью до порядка двух функций от n: $f(n) \gtrsim g(n)$, $f(n) \sim g(n)$ и $f(n) \asymp g(n)$.

Теорема 1. *Теорема 1 (нижняя оценка сложности обратимой схемы). Для любого $n > 0$ верно неравенство*

$$L(n,q) \geqslant \frac{2^n(n-2) - n\log_2(n+q)}{3\log_2(n+q)} \ .$$

Теорема 2. *Следствие 1. Для любого $n > 0$ верно неравенство*

$$D(n,q) \geqslant \frac{2^n(n-2) - n\log_2(n+q)}{3(n+q)\log_2(n+q)} .$$

Доказательство следует из теоремы 1 и соотношения (4).

Теорема 3. *Следствие 2. Для обратимой схемы $\mathfrak{S}$ без дополнительных входов верна следующая нижняя оценка глубины:*

$$D(n,0) \gtrsim \frac{2^n}{3\log_2 n} .$$

Теорема 4. *Теорема 2 (верхняя оценка глубины обратимой схемы). Верны следующие оценки:*

$$D(n,q_1) \lesssim 3n \ \textit{при} \ q_1 \sim 2^n, \ L(\mathfrak{S}) \sim 2^{n+1} ,$$
$$D(n,q_2) \lesssim 2n \ \textit{при} \ q_2 \sim \phi(n)2^n, \ L(\mathfrak{S}) \sim \phi(n)2^{n+1} ,$$

где $\phi(n) < n$ — сколь угодно медленно растущая функция от n.

Теорема 5. *Утверждение. Использование дополнительной памяти в обратимых схемах, состоящих из функциональных элементов множества Ω_n^2, почти всегда позволяет существенно снизить глубину обратимой схемы, в отличие от схем, состоящих из классических необратимых функциональных элементов* [4].

Доказательство следует из теорем 1 и 4.

Мы не оцениваем глубину обратимых схем, реализующих отображения $\mathbb{Z}_2^n \to \mathbb{Z}_2^m$ при $m \neq n$. Тем не менее для таких схем могут быть получены аналогичные оценки глубины путем корректной подстановки параметра m в доказательство теорем 1, 2.

Полученные верхние и нижние оценки глубины обратимой схемы достаточно неточны: они фактически несопоставимы. Так, нижняя оценка глубины при количестве дополнительных входов $q_2 \sim \phi(n)2^n$ из теоремы 4 вырождается в тривиальную $D(n,q_2) \geqslant 0$, в то время как верхняя оценка при данном значении количества дополнительных входов линейна.

К сожалению, вопрос получения эквивалентных с точностью до порядка верхних и нижних оценок для $D(n,q)$ до сих пор остается открытым. Автор надеется, что результаты данной работы станут первым шагом в данном направлении.

4. Нижняя оценка сложности обратимых схем. Перейдем к доказательству первой теоремы.

Доказательство теоремы 1. Докажем при помощи мощностного метода Риордана–Шеннона, что для любого $n > 0$ верно неравенство

$$L(n,q) \geqslant \frac{2^n(n-2) - n\log_2(n+q)}{3\log_2(n+q)} .$$

Пусть $r = |\Omega_n^2|$. Обозначим через $\mathcal{C}^*(n,s) = r^s$ и $\mathcal{C}(n,s)$ количество всех обратимых схем, которые состоят из функциональных элементов множества

Ω_n^2 и сложность которых равна s и не превышает s соответственно. Тогда

$$r = |\Omega_n^2| = \sum_{k=0}^{2} (n-k)\binom{n}{k} = \frac{n^3 - n^2 + 2n}{2} ,$$

$$\frac{n^2(n-1)}{2} + 1 < r \leqslant \frac{n^3}{2} \text{ при } n \geqslant 2 ,$$

$$\mathcal{C}(n,s) = \sum_{i=0}^{s} \mathcal{C}^*(n,i) = \frac{r^{s+1}-1}{r-1} \leqslant \left(\frac{n^3}{2}\right)^{s+1} \cdot \frac{2}{n^2(n-1)} ,$$

$$\mathcal{C}(n,s) \leqslant \left(\frac{n^3}{2}\right)^{s} \cdot \left(1 + \frac{1}{n-1}\right) \text{ при } n \geqslant 2 .$$

Как было сказано ранее, каждой обратимой схеме с $(n+q)$ входами соответствует не более A_{n+q}^n различных булевых отображений $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$. Пусть $s = L(n,q)$, тогда верно следующее неравенство:

$$\mathcal{C}(n+q,s) \cdot A_{n+q}^n \geqslant |F(n,q)| .$$

Поскольку $|F(n,q)| \geqslant |A(\mathbb{Z}_2^n)| = (2^n)!\,/\,2$ и $A_{n+q}^n \leqslant (n+q)^n$, то

$$\left(\frac{(n+q)^3}{2}\right)^{s} \cdot \left(1 + \frac{1}{n+q-1}\right) \cdot (n+q)^n \geqslant (2^n)!\,/\,2 .$$

Несложно убедиться, что при $n > 0$ верно неравенство $(2^n)! > (2^n\,/\,e)^{2^n}$. Следовательно,

$$s(3\log_2(n+q) - 1) + \log_2\left(1 + \frac{1}{n+q-1}\right) + n\log_2(n+q) \geqslant 2^n(n - \log_2 e) ,$$

$$s \geqslant \frac{2^n(n-2) - n\log_2(n+q)}{3\log_2(n+q)} .$$

Из этого неравенства следует утверждение теоремы, поскольку в наших обозначениях $s = L(n,q)$. □

В работе [11] была сделана попытка поднять нижнюю оценку сложности обратимых схем за счет свойства эквивалентности некоторых схем с точки зрения задаваемых ими преобразований. Для этой цели была выдвинута следующая гипотеза о структуре обратимых схем из функциональных элементов множества Ω_n^2.

Гипотеза. *Почти каждая обратимая схема, состоящая из функциональных элементов* NOT, CNOT *и* 2-CNOT *и имеющая* $n \to \infty$ *входов, может быть представлена в виде композиции подсхем сложности* $k = o(n)$ *(кроме последней, у которой сложность* $L \leq k$*), таких, что в каждой подсхеме все элементы являются попарно коммутирующими. Количество обратимых схем, для которых это неверно, пренебрежимо мало.*

К сожалению, в доказательстве этой гипотезы в работе [11] была допущена ошибка: несложно показать, что количество всех обратимых схем сложности выше n, не соответствующих утверждению гипотезы, не является пренебрежимо малым по отношению к общему количеству схем данной сложности.

5. Верхняя оценка глубины обратимых схем без дополнительных входов. В работе [11] предложен алгоритм синтеза обратимой схемы

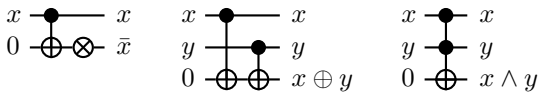

Рис. 2: Выражение функциональных элементов базиса $\{\neg, \oplus, \wedge\}$ через композицию элементов NOT, CNOT и 2-CNOT

$\mathfrak{S}$ без дополнительных входов, задающей подстановку $h \in A(\mathbb{Z}_2^n)$; доказано, что сложность синтезированной схемы удовлетворяет соотношению

$$L(\mathfrak{S}) \lesssim 52n2^n/\log_2 n\ . \tag{5}$$

Очевидно, что $D(\mathfrak{S}) \leqslant L(\mathfrak{S})$, поэтому $D(n,0) \lesssim 52n2^n/\log_2 n$. Однако константу 52 в данной оценке можно уменьшить.

Алгоритм синтеза из работы [11] задает произведение $L \sim \log_2 n$ независимых транспозиций одним элементом k-CNOT и множеством элементов NOT и CNOT с помощью действия сопряжением. Для этого строится матрица из векторов, соответствующих этим транспозициям. В матрице обнуляются некоторые столбцы путем сложения по модулю 2 с совпадающими с ними столбцами (не более $2n$ элементов CNOT), а в конце работы алгоритма почти все столбцы матрицы делаются единичными (не более $2n$ элементов NOT)[2]. Очевидно, что обнулять столбцы матрицы можно с логарифмической глубиной (глубина не более $2\log_2 n$), а элементы NOT можно применять с константной глубиной (глубина не превышает 2).

Если аккуратно заменить в доказательстве оценки (5) из работы [11] величину $4n$, соответствующую сложности описанных выше шагов алгоритма синтеза обратимой схемы, на величину $2(\log_2 n+1)$, то можно получить следующую верхнюю оценку для $D(n,0)$:

$$D(n,0) \lesssim 36n2^n/\log_2 n\ .$$

Однако остается открытым вопрос получения эквивалентных с точностью до порядка нижней и верхней оценок для функции $D(n,0)$.

6. Верхняя оценка глубины обратимых схем с дополнительными входами. О. Б. Лупановым [4] был предложен асимптотически наилучший метод синтеза схем из функциональных элементов с задержками, реализующих булевы функции, в регулярном базисе. Было доказано, что для булевой функции от n переменных и в случае равных единичных задержек всех элементов базиса задержка схемы эквивалентна n. Применим аналогичный подход для получения верхней оценки глубины обратимых схем, состоящих из функциональных элементов множества Ω^2_{n+q} и реализующих заданное отображение $f \in F(n,q)$.

Базис $\{\neg, \oplus, \wedge\}$ является функционально полным, поэтому с его помощью можно реализовать любое отображение $f \in F(n,q)$. Выразим каждый элемент этого базиса через композицию функциональных элементов NOT, CNOT и 2-CNOT (рис. 2). Видно, что каждый элемент реализуется со сложность и глубиной не выше 2, при этом требуется максимум один дополнительный вход.

[2]Коэффициент 2 возникает за счет действия сопряжением.

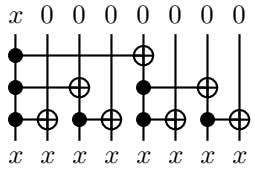

Рис. 3: Копирование значения с одного входа на дополнительные входы с логарифмической глубиной (входы схемы сверху, выходы — снизу)

Отметим также, что если значение с одного входа в дальнейшем должно участвовать в k операциях, то для уменьшения глубины схемы производится копирование этого значения на дополнительные входы, а затем эти дополнительные входы используются в k операциях независимо друг от друга. В итоге можно получить подсхему с глубиной не k, а $(\lceil \log_2 k \rceil + 1)$ (рис. 3).

Докажем следующую лемму о глубине обратимой схемы, реализующей все конъюнкции n переменных вида $x_1^{a_1} \wedge \ldots \wedge x_n^{a_n}$, $a_i \in \mathbb{Z}_2$.

Теорема 6. *Лемма. Все конъюнкции n переменных вида $x_1^{a_1} \wedge \ldots \wedge x_n^{a_n}$, $a_i \in \mathbb{Z}_2$, можно реализовать обратимой схемой $\mathfrak{S}_n$, состоящей из функциональных элементов множества Ω_n^2, имеющей глубину $D(\mathfrak{S}_n) \sim n$ и использующей $q(\mathfrak{S}_n) \sim 3 \cdot 2^n$ дополнительных входов. При этом сложность такой схемы $L(\mathfrak{S}_n) \sim 3 \cdot 2^n$.*

Доказательство. Вначале реализуем все инверсии $\bar{x}_i$, $1 \leqslant i \leqslant n$. Сделать это можно с глубиной $D_1 = 2$ при использовании $L_1 = 2n$ элементов NOT и CNOT и $q_1 = n$ дополнительных входов.

Искомую обратимую схему $\mathfrak{S}_n$ будем строить следующим образом: при помощи схем $\mathfrak{S}_{\lceil n/2 \rceil}$ и $\mathfrak{S}_{\lfloor n/2 \rfloor}$ реализуем все конъюнкции $\lceil n/2 \rceil$ первых и $\lfloor n/2 \rfloor$ последних переменных. Затем реализуем конъюнкции выходов этих двух схем каждого с каждым. Любой выход будет участвовать не более чем в $2 \cdot 2^{n/2}$ конъюнкциях, поэтому получение искомых конъюнкций можно реализовать с глубиной не более чем $(2 + n/2)$, сложностью не более чем $3 \cdot 2^n$ и с использованием не более чем $3 \cdot 2^n$ дополнительных входов.

Таким образом, получаем следующие соотношения:

$$D(\mathfrak{S}_n) \sim \frac{n}{2} + D(\mathfrak{S}_{n/2}) \sim n \ ,$$
$$L(\mathfrak{S}_n) \sim 3 \cdot 2^n + 2L(\mathfrak{S}_{n/2}) \sim 3 \cdot 2^n \ ,$$
$$q(\mathfrak{S}_n) \sim 3 \cdot 2^n + 2q(\mathfrak{S}_{n/2}) \sim 3 \cdot 2^n \ .$$

□

Теперь перейдем непосредственно к доказательству теоремы 4. Основное отличие метода синтеза, описываемого в этом доказательстве, от стандартного метода О. Б. Лупанова заключается в следующем: в обратимых схемах запрещено ветвление входов и выходов, поэтому для получения требуемых оценок для функции $D(n, q)$ активно используются подсхемы по копированию значений с промежуточных выходов на дополнительные входы с логарифмической глубиной (см. рис. 3). Также подсчитывается количество используемых дополнительных входов и получаемая при этом сложность схемы.

Доказательство теоремы 4. Докажем, что для произвольного отображения $f \in F(n,q)$ верны следующие соотношения:

$$D(f,q_1) \lesssim 3n \text{ при } q_1 \sim 2^n,\ L(\mathfrak{S}) \sim 2^{n+1}\ , \tag{6}$$

$$D(f,q_2) \lesssim 2n \text{ при } q_2 \sim \phi(n)2^n,\ L(\mathfrak{S}) \sim \phi(n)2^{n+1}\ , \tag{7}$$

где $\phi(n) < n$ — сколь угодно медленно растущая функция от n.

Булево отображение $f\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ можно представить следующим образом:

$$f(\mathbf{x}) = \bigoplus_{a_{k+1},\ldots,a_n \in \mathbb{Z}_2} x_{k+1}^{a_{k+1}} \wedge \ldots \wedge x_n^{a_n} \wedge f(\langle x_1,\ldots,x_k,a_{k+1},\ldots,a_n\rangle)\ . \tag{8}$$

Каждое из 2^{n-k} отображений $f_i(\langle x_1,\ldots,x_k\rangle) = f(\langle x_1,\ldots,x_k,a_{k+1},\ldots,a_n\rangle)$, где

$$\sum_{j=1}^{n-k} a_{k+j}\cdot 2^{j-1} = i\ ,$$

является отображением $\mathbb{Z}_2^k \to \mathbb{Z}_2^n$. Его можно представить в виде системы n координатных булевых функций $f_{i,j}(\mathbf{x})$, $\mathbf{x} \in \mathbb{Z}_2^k$, $1 \leqslant j \leqslant n$.

Воспользуемся следующим аналогом совершенной дизъюнктивной нормальной формы для булевой функции:

$$f_{i,j}(\mathbf{x}) = \bigoplus_{\substack{\boldsymbol{\sigma}\in\mathbb{Z}_2^k \\ f_{i,j}(\boldsymbol{\sigma})=1}} x_1^{\sigma_1} \wedge \ldots \wedge x_k^{\sigma_k}\ . \tag{9}$$

Разбив все 2^k конъюнкций вида $x_1^{\sigma_1}\wedge\ldots\wedge x_k^{\sigma_k}$ на фиксированные группы, в каждой из которых не более s конъюнкций, получим $p = \lceil 2^k/s\rceil$ групп. Используя конъюнкции одной группы, по формуле (9) можно получить не более 2^s булевых функций. Обозначим множество булевых функций, реализуемых при помощи конъюнкций i-й по счету группы, через G_i, $1 \leqslant i \leqslant p$, тогда $|G_i| \leqslant 2^s$. Теперь мы можем переписать равенство (9) в следующем виде:

$$f_{i,j}(\mathbf{x}) = \bigoplus_{\substack{t=1\ldots p \\ g_{j_t}\in G_t \\ 1\leqslant j_t\leqslant |G_t|}} g_{j_t}(\mathbf{x})\ . \tag{10}$$

Замечание. Все булевы функции множества G_i можно реализовать по тому же принципу, что и все конъюнкции в лемме (разбиение множества входов пополам): глубина полученной подсхемы $D \sim s$, сложность $L \sim 3\cdot 2^s$, количество дополнительных входов $q \sim 2^{s+1}$.

Таким образом, искомая обратимая схема $\mathfrak{S}$, реализующая отображение f, состоит из следующих обратимых подсхем (рис. 4).

1) Подсхема $\mathfrak{S}_1$, реализующая все конъюнкции первых k переменных x_i, согласно лемме, с глубиной $D_1 \sim k$, сложностью $L_1 \sim 3\cdot 2^k$ и $q_1 \sim 3\cdot 2^k$ дополнительными входами.

2) Подсхема $\mathfrak{S}_2$, реализующая все булевы функции $g \in G_i$ для всех $i \in \mathbb{Z}_p$ по формуле (9) с глубиной $D_2 \sim s$, сложностью $L_2 \sim 3p2^s$ и $q_2 \sim$

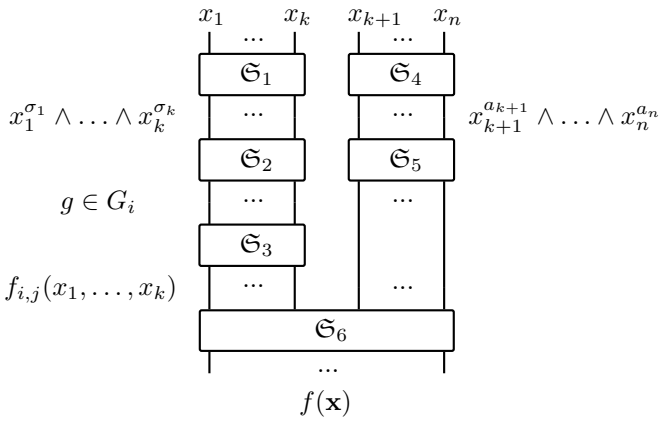

Рис. 4: Структура обратимой схемы $\mathfrak{S}$, реализующей отображение (8) (входы схемы сверху, выходы — снизу)

$p2^{s+1}$ дополнительными входами (см. замечание, касающееся реализации всех булевых функций множества G_i).

3) Подсхема $\mathfrak{S}_3$, реализующая все $n2^{n-k}$ координатных функций $f_{i,j}(\mathbf{x})$, $i \in \mathbb{Z}_{2^{n-k}}$, $j \in \mathbb{Z}_n$, по формуле (10). Особенностью данной подсхемы является то, что некоторая булева функция $g \in G_t$ может использоваться больше одного раза. Максимальное количество использования функции g не превосходит $n2^{n-k}$. Следовательно, сперва нам необходимо скопировать значения с выходов подсхемы $\mathfrak{S}_2$ для всех таких булевых функций. Это можно сделать с глубиной $(n-k+\log_2 n)$, используя не более $pn2^{n-k}$ функциональных элементов и $pn2^{n-k}$ дополнительных входов (см. рис. 3). Затем производится сложение по модулю 2 полученных выходов с глубиной $\log_2 p$, сложностью $(p-1)n2^{n-k}$ и без дополнительных входов. Таким образом, подсхема $\mathfrak{S}_3$ имеет глубину $D_3 \sim n-k+\log_2 p$, сложность $L_3 \sim (2p-1)n2^{n-k}$ и $q_3 \sim pn2^{n-k}$ дополнительных входов.

4) Подсхема $\mathfrak{S}_4$, реализующая все конъюнкции последних $(n-k)$ переменных x_i, согласно лемме, с глубиной $D_4 \sim (n-k)$, сложностью $L_4 \sim 3 \cdot 2^{n-k}$ и $q_4 \sim 3 \cdot 2^{n-k}$ дополнительными входами.

5) Подсхема $\mathfrak{S}_5$, необходимая для копирования $(n-1)$ раз значения каждого выхода подсхемы $\mathfrak{S}_4$. Это можно сделать с глубиной $D_5 \sim \log_2 n$, сложностью $L_5 = (n-1) \cdot 2^{n-k}$ и $q_5 = (n-1)2^{n-k}$ дополнительными входами.

6) Подсхема $\mathfrak{S}_6$, реализующая булево отображение f по формуле (8). Структура данной подсхемы следующая: все $n2^{n-k}$ координатных функций $f_{i,j}(\mathbf{x})$ группируются по 2^{n-k} функций (всего n групп, соответствующих n выходам отображения f). Функции одной группы объединяются по две. В каждой паре функций производится конъюнкция соответствующих выходов подсхем $\mathfrak{S}_3$ и $\mathfrak{S}_5$ при помощи двух элементов 2-CNOT. При этом для каждой пары функций используется один дополнительный вход для хранения промежуточного результата. Таким образом, данный этап требует глубины 2, $n2^{n-k}$ элементов 2-CNOT и $n2^{n-k-1}$ дополнительных входов. Затем в каждой из n групп полученных значений происходит суммирование по подулю 2 при помощи элементов CNOT с логарифмической глубиной. Следовательно, этот этап требует глубины $(n-k-1)$, элементов CNOT в

количестве $n(2^{n-k-1}-1)$ и не использует дополнительные входы, так как можно обойтись уже существующими выходами для суммирования по модулю 2.

В итоге получаем подсхему $\mathfrak{S}_6$ с глубиной $D_6 \sim (n-k)$, сложностью $L_6 \sim 3n2^{n-k-1}$ и $q_6 \sim n2^{n-k-1}$ дополнительными входами.

Отметим, что подсхемы $\mathfrak{S}_1$–$\mathfrak{S}_3$ и $\mathfrak{S}_4$–$\mathfrak{S}_5$ могут работать параллельно, поскольку они работают с непересекающимися подмножествами множества входов $x_1, \ldots, x_n$ обратимой схемы $\mathfrak{S}$ (см. рис. 4).

Будем искать параметры k и s, удовлетворяющие следующим условиям:

$$\begin{cases} k+s=n\ , \\ 1 \leqslant k < n\ , \\ 1 \leqslant s < n\ , \\ 2^k \,/\, s \geqslant \psi(n)\ , \quad \text{где } \psi(n) \text{ — некоторая растущая функция.} \end{cases}$$

В этом случае $p = \lceil 2^k \,/\, s \rceil \sim 2^k \,/\, s$.

Суммируя глубины, сложности и количество дополнительных входов всех подсхем $\mathfrak{S}_1$–$\mathfrak{S}_6$, получаем следующие оценки для характеристик обратимой схемы $\mathfrak{S}$.

Глубина:

$$D(\mathfrak{S}) \sim \max(k+s+n-k+\log_2 p\ ;\ n-k+\log_n)+n-k\ ,$$
$$D(\mathfrak{S}) \sim 2n+s\ .$$

Сложность:

$$L(\mathfrak{S}) \sim 3\cdot 2^k + 3p2^s + (2p-1)n2^{n-k} + 3\cdot 2^{n-k} + n2^{n-k} + 3n2^{n-k-1}\ ,$$
$$L(\mathfrak{S}) \sim 3\cdot\frac{2^n}{2^s} + \frac{3\cdot 2^n}{s} + \frac{n2^{n+1}}{s} \sim \frac{n2^{n+1}}{s}\ .$$

Количество используемых дополнительных входов:

$$q(\mathfrak{S}) \sim 3\cdot 2^k + p2^{s+1} + pn2^{n-k} + 3\cdot 2^{n-k} + n2^{n-k} + n2^{n-k-1}\ ,$$
$$q(\mathfrak{S}) \sim 3\cdot\frac{2^n}{2^s} + \frac{2^{n+1}}{s} + \frac{n2^n}{s} \sim \frac{n2^n}{s}\ .$$

Мы построили обратимую схему $\mathfrak{S}$ для произвольного отображения $f \in F(n,q)$, откуда следует, что $D(n,q) \leqslant D(\mathfrak{S})$.

Оценка (6) достигается при $k = \lceil n \,/\, \phi(n) \rceil$, $s = n - \lceil n \,/\, \phi(n) \rceil$, где $\phi(n) \leqslant n\,/(\log_2 n + \log_2 \psi(n))$ и $\psi(n)$ — любые сколь угодно медленно растущие функции.

Оценка (7) достигается при $k = n - \lceil n \,/\, \phi(n) \rceil$, $s = \lceil n \,/\, \phi(n) \rceil$, где $\phi(n) < n$ — сколь угодно медленно растущая функция. □

Остается открытым вопрос получения эквивалентных с точностью до порядка нижней и верхней оценок для функции $D(n,q)$ в случае $q \to \infty$.

7. Заключение. В работе рассмотрен вопрос о глубине обратимых схем, состоящих из функциональных элементов NOT, CNOT и 2-CNOT. Изучена функция Шеннона $D(n,q)$ глубины обратимой схемы, реализующей какое-либо отображение $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ из множества $F(n,q)$, как функции от n и количества дополнительных входов схемы q. Доказаны некоторые нижние и верхние асимптотические оценки функции $D(n,q)$ для обратимых схем

с дополнительными входами и без. Показано, что использование дополнительной памяти в таких обратимых схемах почти всегда позволяет снизить глубину схемы, в отличие от схем, состоящих из классических необратимых функциональных элементов.

При решении задачи синтеза обратимой схемы, реализующей какое-либо отображение, приходится искать компромисс между сложностью синтезированной схемы, ее временем работы (глубина схемы) и количеством используемой дополнительной памяти (дополнительных входов в схеме). Направлением дальнейших исследований является более детальное изучение зависимости этих величин друг от друга.

Список литературы

[1] Shannon C. E. The synthesis of two-terminal switching circuits // Bell System Techn. J. 1949. **28**, N 8. 59–98.

[2] Лупанов О. Б. Об одном методе синтеза схем // Изв. вузов. Радиофизика. 1958. **1**, № 1. 23–26.

[3] Карпова Н. А. О вычислениях с ограниченной памятью // Математические вопросы кибернетики. Вып. 2. М.: Наука, 1989. 131–144.

[4] Лупанов О. Б. О схемах из функциональных элементов с задержками // Проблемы кибернетики. Вып. 23. М.: Наука, 1970. 43–81.

[5] Храпченко В. М. Новые соотношения между глубиной и задержкой // Дискрет. матем. 1995. **7**, № 4. 77–85.

[6] Закаблуков Д. В. Быстрый алгоритм синтеза обратимых схем на основе теории групп подстановок // Прикл. дискрет. матем. 2014. № 2. 101–109.

[7] Shende V. V., Prasad A. K., Markov I. L., Hayes J. P. Synthesis of reversible logic circuits // IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 2006. **22**, N 6. 710–722. DOI: 10.1109/TCAD.2003.811448.

[8] Закаблуков Д. В., Жуков А. Е. Исследование схем из обратимых логических элементов // Информатика и системы управления в XXI веке: Сб. тр. №9 молодых ученых, аспирантов и студентов. М.: МГТУ им. Н. Э. Баумана, 2012. 148–157.

[9] Винокуров С. Ф., Францева А. С. Приближенный алгоритм вычисления сложности обратимой функции в базисе Тоффоли // Изв. Иркут. гос. ун-та. Сер. матем. 2011. **4**, № 4. 12–26.

[10] Maslov D. A., Dueck G. W., Miller D. M. Techniques for the synthesis of reversible Toffoli networks // ACM Trans. Design Automat. Electron. Syst. 2007. **12**, N 4. DOI: 10.1145/1278349.1278355.

[11] Закаблуков Д. В. Вентильная сложность обратимых схем как мера сложности четных подстановок // Вестн. МГТУ им. Н. Э. Баумана. Сер. приборостр. 2015. № 1. 67–82.

[12] Abdessaied N., Wille R., Soeken M., Drechsler R. Reducing the depth of quantum circuits using additional circuit lines // Proc. 5th Int. Conf. Reversible Computation. Victoria, BC, Canada, 2013. 221–233. DOI: 10.1007/978-3-642-38986-3_18.

[13] Toffoli T. Reversible Computing // Automata, Languages and Programming. Ser. Lect. Notes Comput. Sci. Berlin; Heidelberg: Springer, 1980. Vol. 85. 632–644. DOI: 10.1007/3-540-10003-2_104.

[14] Maslov D. A. Reversible Logic Synthesis: Ph. D. Thesis. 2003. URL: http://web.cecs.pdx.edu/~mperkows/PerkowskiGoogle/thesis_maslov.pdf